BY ORDER OF THE
43D AIRLIFT WING COMMANDER

POPE AFB INSTRUCTION 33-108

1 JUNE 2000

Communications and Information

METROPOLITAN AREA NETWORK SECURITY POLICY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO/PP WWW site at: **http://afpubs.hq.af.mil.**

OPR: 43 CS/SCBS (SMSgt Sanders)

Certified by: 43 CS/CC (Major Perkins)
Pages: 32
Distribution: F

This instruction applies to all users of the Metropolitan Area Network (MAN) on Pope AFB. This instruction implements Air Force Policy Directive 33-2, *Information Protection*; Air Force Instruction (AFI) 33-112, *Computer Systems Management,* AFI 33-115V1, *Network Management,* AFI 33-129, *Transmission of Information Via the Internet,* AFI 33-202, *Computer Security,* AFI 33-204, *Information Protection Security Awareness, Training, and Education (SATE) Program,* Air Force Manual (AFMAN) 33-223, *Identification and Authentication, and* Air Force Systems Security Instruction (AFSSI) 5024, Volume 1, *The Certification and Accreditation (C&A) Process.*

1. General.

1.1. Introduction. Computer Security (COMPUSEC) protects your computer and everything associated with it. Most importantly, COMPUSEC protects the information you've stored in your system. All users of the systems and information contained therein must share the responsibility for the security, integrity, and confidentiality of the systems and the information. COMPUSEC is achieved by complying with this instruction.

1.2. Purpose. This document establishes system security for the base metropolitan area network (MAN), defines network security directives, and specifies required security countermeasures. This instruction also addresses the minimum security measures for systems interfacing with the MAN. Specifically, this document defines the network security measures to ensure security, confidentiality, and integrity of information obtained, created, or maintained by the MAN, and assures its service availability. Information includes all electronically stored and printed files contained on servers, micro- and minicomputers, and mainframes. Failure to observe the prohibitions and mandatory provisions in this publication, whether they apply to Pope AFB specifically or are dictated by higher directives, is a violation of Article 92, UCMJ, and noncompliance may result in punishment under Article 92, UCMJ.

1.3. Mission. The mission of the MAN is to support the electronic creation, transfer, sharing, and presentation of information by using networked personal computers and commercial off-the-shelf software. The MAN is a general purpose, multi-user system used by the 43d Airlift Wing (43 AW), and its groups and squadrons, all wing agencies, and tenant units. It provides access to a myriad of electronic services (such as electronic mail [e-mail], word processing, spreadsheets, electronic forms, and databases) and a gateway to the Internet. As a result, the MAN provides users with the tools to improve business processes, resulting in increased efficiency and effectiveness. Therefore, this document was developed to provide MAN users and administrators with a pragmatic security directive, realistic guidelines, and the tools necessary to accomplish their mission.

1.4. Applicability and Scope. This security directive provides the minimum MAN computer security requirements and establishes the set of rules and practices to regulate management, protection, and distribution of data entrusted to the network. The policies stated in this instruction apply to everyone administering and using the MAN.

1.5. Relationship to Other Publications. The National Computer Security Center (NCSC) Standards and Guides (Rainbow-series), Department of Defense (DoD) Directives, Air Force Systems Security Instructions (AFSSIs), Air Force Instructions (AFIs), and Air Force Systems Security Memorandums (AFSSMs) govern the operation and management of information systems.

1.5.1. Conflicting Guidance. The provisions of this security instruction do not replace the requirements contained in Air Force and DoD-level documents. If there is a conflict, the requirements in higher-level regulations govern. Report the conflict to your Wing Information Assurance Manager.

1.6. Basic System Facts. The following basic system information describes the MAN.

1.6.1. Authorized Data on the MAN. The MAN will not be used to process classified information without an encryption device that has been approved by the Wing Information Assurance Office and the Network Control Center. Classified information will only be sent and received via the Secret Internet Protocol Network (SIPRNET). Sensitive information is the highest level of data authorized on the MAN. Typically, sensitive information includes, but is not limited to, that pro-

tected by the Privacy Act of 1974, privileged data, proprietary data, and For Official Use Only (FOUO) data.

1.6.2. Minimum User Clearances. Access to the MAN does not require a security clearance. MAN access is based on the key concepts of "authorization" and "need-to-know." Authorization is validated when an authorized functional system administrator (FSA) notifies the Network Control Center (NCC) that an individual requires MAN access to perform official duties and that a personal user ID (PUID) should be issued. Need-to-know access to unclassified or sensitive information must be based on either an explicit written authorization or implicit authorization derived from the individual's official duty assignment. Additionally, government contractors will not be given access to any information accessible on the MAN unless first approved through proper channels. Approval for contractor access will be worked through the appropriate contracting officer and approved only when required to satisfy the terms of the contract. The contracting office is responsible for obtaining appropriate nondisclosure agreements and for ensuring the requirements of the Privacy Act of 1974 and other laws protecting various information are enforced when it is necessary for contractors to have access to sensitive information on the MAN.

1.7. Roles and Responsibilities.

1.7.1. Designated Approval Authority (DAA). The DAA for the Pope MAN assumes responsibility for operating the MAN, determines the acceptable level of risk at which the system will operate, and has the authority to allocate resources to achieve an acceptable level of security. The DAA is responsible to provide authorization for connection of systems and networks to the MAN and is the only person authorized to accredit the system. The DAA for the Pope AFB MAN is the 43 CS/CC. Each unit or directorate commander is the DAA for assets within their unit.

1.7.2. Wing Information Assurance Office (WIAO). The WIAO is responsible for managing and implementing Computer Security (COMPUSEC) on Pope AFB. This includes: ensuring initial/annual training, maintaining accreditation information, establishing local policy and procedures, and identifying and ensuring corrective actions on known vulnerabilities. The Wing Information Assurance Office is assigned to 43 CS/SCBS.

1.7.3. Unit Computer Manager (UCM). The UCM is the single COMPUSEC liaison between the unit and the WIAO. The UCM establishes unit standardization and reporting controls for the unit as specified by the DAA and implements a unit COMPUSEC program to ensure compliance with the provisions of this instruction. This includes tracking system accreditation, ensuring training, distribution of advisories and tracking of advisory implementation as described in this instruction.

1.7.3.1. Unit Computer System Security Officers (CSSO). If necessary, units may appoint CSSOs to assist the UCM in ensuring the provisions of all applicable security directives are implemented throughout the life cycle of their systems.

1.7.4. Network Control Center (NCC). The NCC manages infrastructure of the MAN from the interface of the user's terminal to the interface(s) of the base-level host, base-level server, or transmission system providing connectivity to off-base assets and includes all the base network backbone infrastructure components. They manage and configure all hardware on the backbone including routers, switches, hubs, multi-plexers, serial link modems, media converters, circuits, repeaters, bridges, gateways, software, configuration and user management of Pope Domain servers etc.

1.7.4.1. Help Desk. The primary interface between unit Functional System Administrators

(FSAs) and the Network Control Center. The 43 CS Help Desk is tasked to receive trouble calls, open trouble tickets, assess and resolve problems, record fault-isolation procedures, close trouble tickets within defined response times, and report the status of problem and resolution actions to the affected customer(s). Provides a central repository for technical advice and solutions for network systems. Problems which Help Desk technicians are not trained or equipped to handle are routed to the appropriate office for resolution. The Help Desk is the central hub for all base network problems. Customers must go through their Functional System Administrator for problem resolution. Only authorized functional system administrators, who have been appointed in writing, are allowed to submit trouble calls to the Help Desk. FSAs may report problems by calling 394-2622 or e-mailing ncc.helpdesk@pope.af.mil.

1.7.5. Functional System Administrator (FSA). FSAs provide oversight and management of servers and workstations for the area to which they are assigned. They receive overall guidance from the NCC. FSAs must thoroughly understand the customer's mission and be completely knowledgeable of the hardware and software capabilities/limitations. The FSA's area of responsibility is from the user's terminal to the server but does not include the network backbone infrastructure components. FSAs ensure servers, workstations; peripherals, communication devices, and software are on-line and available to support customers. They work directly with Work Group Managers and individual users from initial set up through final disposition of each account.

1.7.5.1. Workgroup Managers (WGMs). WGMs provide immediate support to users for resolving workstation problems and managing and protecting electronic records in accordance with prescribing directives and public law. They are responsible for all support activities pertaining to single client workstations, not server administration. (Server administration will either be provided by FSAs in the organizations or NCC personnel.) WGMs take direction and receive support from their FSAs or, when beyond their capabilities, the NCC. WGMs must go through the unit FSAs in order to report problems to the Help Desk in the NCC. With WGMs managing business processes and user clients, FSAs and network communications personnel are able to focus on higher level support requirements of optimizing functional system applications support and network performance for all users.

1.7.6. Unit Commanders. Each unit commander has overall responsibility for proper management of MAN resources under their control. They validate all requests for access to the network and appoint all system and security personnel (UCMs and FSAs) for their unit. Unit commanders also serve as Designated Approval Authorities (DAAs).

1.7.7. User (Customer): Each MAN user must follow established security directives and procedures, safeguard sensitive data and critical resources, and mark output products appropriately (i.e., FOUO, Privacy Act, etc.). All users must complete Security Awareness Training and Education (SATE) training within 30 days of being given access to information systems. Users report security problems or incidents through the WGM or the FSA to the Wing Information Assurance Office as soon as possible after detection.

2. Operational Security Directives.

2.1. Assurance. Assurance is the measure of confidence that the security features and architecture of the MAN accurately mediates and enforces the security directives. Assurance is established by the certification and accreditation (C&A) of the MAN and is maintained through compliance with this document; AFI 33-202, *The Computer Security (COMPUSEC) Program*; AFSSI 5024, Volume I, *The*

Certification and Accreditation Process; and AFSSI 5024, Volume II, *The Certifying Official's Handbook.* Additional information can be found in paragraph **2.13.** of this instruction.

2.2. Accountability. IAW AFSSI 5027, *Network Security Policy*, the MAN operating system software will maintain an automated audit trail that can be used to report COMPUSEC-related activities. This will ensure people with access to the MAN can be held accountable for their actions. Only a subset of all available MAN auditable events will be activated for full-time auditing. The focus used to select the auditable events is based on providing the ability to monitor specific security features and is primarily directed at auditing the granting and modification of user security rights and security attributes. Although FSAs will be audited in greater detail due to their supervisory privileges, all MAN users will be audited to some degree to include events such as logging in and out of the MAN. Additionally, the FSA will terminate access when unauthorized user activity is detected. The audit trail will be of sufficient detail to reconstruct events to determine the cause or magnitude of compromise should a security violation or malfunction occur. The Wing Information Assurance Office (WIAO) will review the audit trail data. Retention of audit records that cover periods involving a security incident will be in accordance with appropriate disposition record requirements.

2.2.1. Auditable Events. The following comprise auditable events:

2.2.1.1. Use of account log-in and log-out.

2.2.1.2. Actions to create, modify, copy, execute, or delete programs, directories, or files.

2.2.1.3. Actions taken by FSAs, UCMs, and work group Managers (WGMs). Examples include adding a user, changing user rights, or performing file server restarts.

2.2.1.4. Any event that attempts to change the security profile of the system. Examples include changing access controls (rights or attributes) to files, directories, and user discretionary access, or changing a user password.

2.2.1.5. Any event that attempts to violate the security directives of the system. Examples include too many attempts to log-in or attempts to violate the access control limits of a device.

2.2.1.6. Passwords, or character strings incorrectly given as passwords that might possibly expose the password, shall not be recorded in the audit trail.

2.2.2. Specific Audit Information. The audit trail will record the following minimum information for each auditable event. Only the WIAO can grant authorization for FSAs to disable auditing or change their configured audit mechanisms.

2.2.2.1. Date and time of the event.

2.2.2.2. Unique identifier of the user or device generating the event.

2.2.2.3. Type of event.

2.2.2.4. Success or failure of the event.

2.2.2.5. Origin (terminal ID) of the request for identification and authentication events.

2.2.2.6. Name of the program or file introduced, addressed, or deleted.

2.2.2.7. Description of actions taken by the FSAs and computer system security officers.

2.2.3. Audit Review. The WIAO office will randomly review audit data. They will review the following: patterns of access to individual objects, access histories of specific processes and users,

use of various protection mechanisms and effectiveness, repeated attempts to bypass protection mechanisms, and monitor use of privileges.

2.2.4. Protection of Audit Files. Audit data files and products will be protected as sensitive information.

2.2.5. Events Selected for Audit. A subset of all available MAN events subject to auditing will be selected for auditing. These events are primarily directed at the assignment and modification of a user's rights and attributes.

2.2.6. Internet Security Scans (ISS). The Wing Information Assurance Office (WIAO) will run ISS on a monthly basis to identify any network vulnerabilities. A list of all vulnerabilities by Internet Protocol address along with corrective action will be provided to the affected Unit Computer Security Manager. The UCM will work with the Functional System Administrators to ensure corrective actions are taken. The UCM will report compliance to the WIAO.

2.3. Access Control.

2.3.1. Method of Access Control. A combination of physical security, personnel security, and system security mechanisms will be used to control access to the MAN. Users must properly identify and authenticate before accessing the MAN. The method of access control for the MAN is a combination of a personal user login ID (identification) and a unique password (authentication).

2.3.2. Identification.

2.3.2.1. Personal Accounts. Users will request accounts through their FSAs. MAN users must complete a Personal User ID (PUID) Receipt (**Attachment 2**) when they receive their personal user ID and initial account password. By completing the PUID Receipt, the user agrees to comply with all MAN security requirements. MAN users agree to complete Security Awareness Training and Education (SATE) training within 30 days of receipt of their User ID. Failure to do so will result in the account being disabled. Unit Computer Security Managers will maintain the PUID receipt along with documentation of SATE training. See the NCC for additional guidance on establishing a personal account.

2.3.2.2. Closing User ID Accounts. MAN user ID accounts and passwords will be deleted within one duty day of the user's departure from an organization, or when a user no longer requires access to perform official duties. If authorized, the FSA will remove the account. If not, the FSA will notify the NCC to remove the account. Units must ensure removal of e-mail accounts is part of the outprocessing steps for personnel. The NCC will conduct quarterly audits to identify dormant accounts. The UCM will be contacted prior to removing dormant to ensure that the account warrants removal.

2.3.3. Authentication. All user login attempts must be authenticated by use of a password.

2.3.3.1. Password Policy. Each user is responsible for observing the basic criteria of good password management: password composition and length, periodic change, ownership, distribution, entry and safeguarding. Users violating this policy endanger everyone's data and may be denied access to network resources.

2.3.3.2. Password creation guidelines. Passwords must be at least 8 characters long. Passwords must contain a mixed combination of at least one letter, at least one number, and at least one special character. A mixed combination means that you cannot simply use an ordinary

word with a string of numbers and special characters tacked on to the beginning or end, i.e. "happy#123" is not an acceptable password.

Character Examples:

Letters = abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

Numbers = 1234567890

Special Characters =! @#$%^&*()_+-={}|[]\:";'<>?,./

Passwords must *not* use ordinary, unchanged "dictionary" words.

If a word can be found in a dictionary or other written matter it can not be used unless it has been significantly changed. This includes but is not limited to names (including nicknames and names of fictional characters), profanity, slang or technical terms, etc.

Significant changes include misspelling, insertion of numbers and special characters, and using multiple words.

Misspelling: You must *significantly* misspell the password. Simply changing one or two letters is not sufficient. Spelling words phonetically is recommended. Example: Change "computer" to "kompewtur" *not* "komputer". (Remember that you still required to use numbers and special characters.)

Adding numbers and characters: You can strengthen passwords by adding numbers and special characters to the *middle* of the password. Do not simply add characters to the beginning or end of the password. Example: Change "telephone" to "tele_9phone" *not* "telephone_9".

Using multiple words: You can use more than one word in your password. Try to use words with at least three letters. Try to separate your words with numbers and special characters; do not simply tack them on to the ends of your password. Good Examples: "run4#cake", "orange8*alert", and "1book&worm". Bad Examples: "apassword-1", "#1bigdog".

Passwords must not be based on personal information. This includes but is not limited to birthdays, license plates, nicknames, names of pets, favorite sports teams, activities, or hobbies, etc.

Password protection guidelines include but are not limited to:

2.3.3.3. Password Life Cycle. Passwords must be changed every 90 days at a minimum. Reusing passwords is strongly discouraged. Previously used passwords may not be re-used for a period of at least six months. Additionally, you are not permitted to reuse your last five passwords. Passwords that have administrator-level access should be changed at least every 60 days.

2.3.3.4. Password Protection. Passwords must not be written down. Users are not permitted to keep written copies of passwords on their person or in their work area. Exception: Passwords may be written down for archival or disaster recovery purposes if strong measures are taken to ensure they are not compromised. This would typically mean sealed envelopes in a safe. Passwords must not be shared or revealed. Multiple users are not permitted to use the same password. Users must not tell anyone else what their password is. Your Pope network password is restricted to logging in to the Pope network; do not use it to log in to any commercial services such as AOL or hotmail. *No one* is authorized to ask a user what his or her password is. Administrators do not need to know what a password is to perform password maintenance.

2.3.3.5. Screen Saver passwords. Do not leave a logged-in computer without securing it. If you are logged in to your computer and leave it, you must secure it by either locking it or activating a password-protected screensaver. The screensaver must be set to activate in 5 minutes or less.

2.3.3.6. Reporting Password compromises. Report any of the following incidents to the Wing Information Assurance Office (WIAO):

If you know or suspect that any password has been compromised.

If someone attempts to convince you to give them your password. This is typically done via telephone. Remember that *no one* is authorized to ask you for your password.

2.3.3.7. Grace Logins. Use of an expired password is not authorized. Users will be restricted to three-grace logins following the expiration of their password. During the grace login, users will be prompted to select a new password.

2.3.3.7.1. Password Lockouts. Users will be allowed three attempts to properly enter their password. A user ID will be locked-out after three unsuccessful password authentication attempts. All MAN users, to include personnel who are on TDY status, will contact their FSA when they are locked-out from their account. The FSA will in-turn contact the 43 CS Help Desk at 394-2622 to unlock the user account. FSA involvement is necessary to verify the request is coming from an authorized MAN account user.

2.3.3.7.2. Automated Password Entry. Password entry will not be automated. For example, do not place your password in a login script or batch file. If you use a program that caches or automatically stores passwords, the Password caching feature must be disabled.

2.3.3.7.3. Broken Passwords. The Wing Information Assurance Office will run a scan of all passwords at least quarterly. If any passwords are broken the following applies:

2.3.3.7.3.1. First Offense: The first time a user's password is broken, the individual will receive a warning. The individual’s password will be reset and 43 CS/CC will notify the user's commander.

2.3.3.7.3.2. Second Offense: If an individual’s password is broken for a second time, the individual will be locked out of the network and 43 CS/CC will notify the user's commander. The user's commander will be required to write/endorse a letter to the 43 SPTG/CC requesting reinstatement.

2.3.3.7.3.3. Any subsequent offenses will result in permanent removal of access to Pope AFB information systems.

2.3.4. Anti-Virus Policy.

2.3.4.1. Software. All systems will have anti-virus software installed. In order to standardize all Pope MAN systems and ensure appropriate updates, the only supported software is Norton Anti-Virus. Additionally, auto-protect must be enabled to ensure continuous scanning of files. Software and instructions are available on the Wing Information Assurance Office (WIAO) web page: (http://popenet/43SPTG/43cs/scb/IA/WIPOHomePage/norton.htm).

2.3.4.1.1. Home Use. Use of government purchased anti-viral software for use on home computers that will be used to create government official files is approved. The WIAO will only provide support and updates for Norton Anti-Virus, however, individuals who use McAfee anti-viral software on their home computers may obtain updates from the DOD Computer Emergency ResponseTeam website at http://199.211.123.12//.

2.3.4.2. Updates. UCMs will be notified when there is an update to the current anti-virus files. They will coordinate with the FSAs in their unit to ensure all systems in their units download this update. This can be accomplished by using the live update option provided the system is obtaining the live update directly from the Pope server. Otherwise update files may be downloaded from the WIAO Web page and manually installed.

2.3.4.3. Reporting Viruses and other Malicious Logic. Upon detecting a suspected or actual malicious logic infection, the user must immediately notify their Unit Computer Manager (UCM) or FSA. If able, the user will remove the virus using Norton anti-virus software. If necessary the UCM or FSA will assist. Upon discovery of a virus, a formal virus incident report (**Attachment 4**) will be sent to the WIAO. Therefore, pertinent viral information should be recorded at the time the virus is detected and removed. The WIAO will forward the report to HQ AMC if necessary.

2.3.4.4. Mail scanning. The NCC will run anti-virus software on the gateway to scan incoming and outgoing email traffic for potential viruses and malicious logic.

2.3.5. Email Use.

2.3.5.1. Only NCC approved email software will be used over the Pope MAN. Approved products are MS Exchange, Outlook 95 or Outlook 97.

2.3.5.2. Email is provided to conduct official business. AFI 33-119, *Electronic Mail* (Email) Management and Use, provides a detailed listing of the allowable uses of DoD email systems for personal use (e.g. what you can use a government telephone for applies to e-mail).

2.3.5.2.1. GI Mail. Global Internet Mail (GI Mail) was designed for non-mission critical operations, with emphasis on morale communications among family members, friends, and co-workers of deployed members. It is a full featured web based e-mail system allowing access from any web browser within the .mil network. Due to obvious OPSEC vulnerabilities GI Mail is AMCs preferred method of electronic mailing (e-mail). The primary goals of the system are to provide a full set of email features to Air Force users worldwide and provide access from any standard web browser, such as Netscape Navigator or Microsoft Internet Explorer. To access GI Mail use Internet Explorer or Netscape and go to “www.gimail.af.mil.” The first time a user accesses GI Mail they must register for an account on the system. Any questions regarding GI Mail can be forwarded to the WIAO.

2.3.5.3. Personal e-mail should not be of such frequency as to interfere with official business.

2.3.5.4. Under no circumstances will chain letters, soliciting, pornography, unofficial advertising or other uses that are incompatible with public service be originated or forwarded from government e-mail systems.

2.3.5.5. All formal or informal e-mail sent or received on DoD owned computer systems is considered official and subject to monitoring. It is subject to the same guidelines as other forms of official Air Force written communication and requires coordination through your

chain of command.

2.3.5.6. It is never permissible to use someone else's identity (userid) and password without proper authority.

2.3.5.7. Users must get permission from their commander before subscribing to or participating in email listservers that are not official Air Force internal information products.

2.3.5.8. E-mail will not be sent directly to everyone on the Global Address List. Information should be forwarded to unit orderly rooms, first sergeants, or commanders for distribution to their personnel.

2.3.5.9. Professional Courtesies.

2.3.5.9.1. Acceptable use of e-mail is based on common sense, common decency, and civility applied to the electronic communications environment.

2.3.5.9.2. E-mail is a means to further the mission by providing services that are efficient, complete, accurate, and timely.

2.3.5.9.3. Place as much information as possible in the subject line of your e-mail. If the e-mail is referencing a meeting of the Functional System Administrators (FSAs) let the recipients know up front (ex. SUBJ: FSA Meeting, 0900/15 Feb 2000, Base Theater).

2.3.5.9.4. If a message is unavoidably long, let the recipients know in the beginning and consider ways to summarize the contents to make the reader's job easier.

2.3.5.9.5. Always include a signature block at the end of official e-mail to ensure all recipients can identify the originator.

2.3.5.9.6. Refrain from using unprofessional language and limit the use of sarcasm and humor.

2.3.5.9.7. Capitalize only to accentuate a word or phrase; typing in capital letters gives people the impression that you are shouting at them.

2.3.5.9.8. It is up to each individual to act responsibly and exercise professionalism and respect for others in the use of the email system. Clarity, brevity, and courtesy are keys to effective written communication.

2.3.5.10. E-mail and Records Management.

2.3.5.10.1. Do not use e-mail files or Internet pages to store official record copies of documents unless they contain an electronic record management application that manages the disposition of the records. Manage records according to AFMAN 37-123, *Management of Records*; AFI 37-138, *Records Disposition—Procedures and Responsibilities*; and AFMAN 37-139, *Records Disposition Schedule*.

2.3.5.11. Information about e-mail. Direct questions concerning the proper use of e-mail to the Wing Information Assurance office, 424-2262/1429.

2.3.6. Network Connection.

2.3.6.1. Modem Connections. Modems are not allowed to connect to the base MAN. Users will access the MAN primarily through on-base terminals or through the NCC Remote Access Server. Users wishing to access the MAN through use of modems must meet specific mission

requirements. Mission needs will be dictated by the unit Designated Approval Authority (DAA) and ultimately approved by the 43 CS/CC. Users must submit such requests in writing through their flight chief, branch chief, or higher level authority and then coordinate the request through their UCM, commander or staff agency chief, and finally to 43 CS/SCBBN. If approved, 43 CS/SCBBN will issue a separate login ID and password for modem users, distinct from their base MAN account. All such connections must comply with all MAN user identification and authentication requirements and AFMAN 33-223. Annually, UCMs will reevaluate the need for modem access that is granted. The NCC will also run a quarterly scan to detect modems. Results will be compared with the list of authorized modems and reported to the AMC Network Operations and Security Center and 43 CS/CC.

2.3.6.2. New Network Connections. Requests for new network connections will be submitted via AF Form 3215. The NCC will conduct a technical analysis of the request and approve or disapprove the request. Prior to connecting any equipment to the new network connections, all certification and accreditation must be completed and all equipment must be properly listed in the Information Processing Management System.

2.3.6.3. Internet Protocol (IP) Addresses. Each authorized user will have an established IP address. The unauthorized use or change of an IP address is prohibited without prior coordination with the NCC at 394-2622. Violations will result in termination of the offending user's access to the MAN with reinstatement only by written request of the user's unit commander or staff agency chief. FSAs will maintain a list of IPs and the associated workstations.

2.3.6.4. Warning Banner. All information systems must display, to each user attempting use or access, a warning about unauthorized use of DoD computer systems and consent to monitoring statement. See **Attachment 4** for the mandatory banner statement. The banner's language should not be expected to change often, but only when deemed necessary by DoD or the Defense Information Systems Agency (DISA). Wing IA will notify the appropriate personnel (i.e., NCC, FSAs and UCMs) when login banner changes are made.

2.3.7. Service Level Agreements. A Service Level Agreement (SLA) must be established between the NCC and the each unit delineating roles and responsibilities for both the NCC and the customer in terms of system administration, manning, funding, and customer support.

2.4. Personnel Security.

2.4.1. Security Clearances. Access to the MAN does not require a security clearance. However, personnel who have their security clearance suspended or revoked for cause, or receive administrative punishment (e.g., Article 15) will have their access eligibility to the MAN reviewed by the unit security manager and commander or staff agency chief. Once a determination has been made to deny access to the MAN, the FSA will be notified and, in turn, he or she will notify the NCC, ensuring MAN access is revoked.

2.5. Hardware.

2.5.1. File Server Access. Physical access to MAN file servers will be restricted by locating them in a climate-controlled, lockable enclosure such as a room, closet or cabinet. Access will be limited to authorized personnel only, such as FSAs and authorized maintenance personnel. All file servers must have a certification and accreditation on file as defined in paragraph **2.13.** Unit Computer Security Managers and Functional Systems Administrators will ensure that servers remain

current with all required patches, anti-viral software updates and any other Wing Information Assurance Office directed software.

2.5.2. Resource Protection. The first line of defense for protecting valuable assets is resource protection. To prevent misuse, abuse, or theft, system hardware will be located in facilities, which can be physically secured or locked.

2.5.3. Hardware Inventory. Organizational equipment control officers (ECOs) will ensure that all hardware assets under their control are listed in the automated data processing equipment Information Processing Management System (IPMS). The NCC will accomplish this task for MAN-wide assets. Organizational ECOs and WIAO personnel will ensure the MAN accreditation control number is associated with each IPMS MAN equipment record. ECOs must ensure that an accreditation number is assigned before equipment is placed in operational use.

2.5.4. Hardware Maintenance. Only authorized maintenance personnel (e.g., NCC personnel, FSAs, and government-approved vendors) will perform hardware maintenance on MAN equipment and workstations. Individual MAN users will not perform hardware maintenance or modifications without the express approval of the NCC. Additionally, vendor maintenance personnel will not be given unescorted access to sensitive information storage media or products during the repair or testing of system components.

2.6. Software.

2.6.1. Making Backup Copies of Original Network Software. The NCC will make backup copies of all original network software that is installed as “standard” on all MAN core servers. FSAs will make backup copies of all original network software that is installed as a “unique” requirement on their file servers and work stations they maintain. Backup copies will be stored separately (preferably off-site) from the master copies whenever possible. They should be stored under lock and key due to the high pilferability of the software. Any duplication of commercially licensed software, except for backup purposes, is a violation of Federal copyright laws.

2.6.2. Archiving (Backup) of MAN File Server Files. At a minimum, a daily incremental backup will be made for data files on each MAN core server. It is strongly recommended that FSAs perform these same backups on their file servers.

2.6.3. Archiving (Backup) of User Files. Users are encouraged to periodically backup their personal files. This is especially true for data files which are located on their workstation hard drive (i.e., C drive), since workstation files are not backed up in any way by the MAN file server backup process.

2.6.4. Unauthorized Software. Only government approved software is authorized on the MAN. Games and pornographic software is unauthorized and will not be installed on any computer or file server. All network operating system and application software that specifically interacts with the MAN, but is not provided to units by official Air Force channels, must be approved by AMC Computer Systems Squadron prior to its implementation. This also applies to freeware and shareware. Requests for approval will be submitted on AF Form 3215 to the Wing Information Assurance Office.

2.6.5. Unauthorized services. Dial-up access to Internet service providers, such as America Online (AOL), CompuServe, or others, is prohibited. Personnel will not participate in “chat lines” or open forum discussions. Guidance on specific network infrastructure services and protocols

policy (for services such as SNMP, SMTP, TELNET etc.) can be found in Chapter 6 of AFSSI 5027.

2.6.6. Using Government Owned Software for Personal Projects. DAAs, group or unit commanders, or staff agency chiefs must approve any use of government computer equipment for personal educational projects, job hunting, or similar uses. Use of government purchased anti-viral software for use on home computers that will be used to create government official files is approved.

2.7. Marking/Labeling.

2.7.1. Labeling Removable Storage Media. Labels will be applied to all removable storage media (i.e. floppy diskettes and tapes) IAW AFSSI 5027, para 5.6. Standard Form 711, **Data Descriptor**, will be used whenever possible. If SF Form 711 is not available for use, the original labels that came with the media may be used. Either label will indicate the storage media's owner (by name or office symbol), use, and description of contents. Additionally, appropriate markings must be indicated on the label of all removable magnetic storage media that contains sensitive information. AFVA 33-207, *Privacy Act Label*, may be used to indicate the storage media containing personal data. All removable media will have one of the following classification labels: SF 706-**TOP SECRET**, SF 707-**SECRET**, SF 708-**CONFIDENTIAL**, or SF 710-**UNCLASSIFIED**.

2.7.2. Marking/Labeling Controlled Unclassified Information. "FOUO," "Sensitive But Unclassified" information, and "Sensitive Information," as defined by the Computer Security Act of 1987, fall into the category of "unclassified controlled information." These types of information will be marked/labeled IAW DoD5200.1-R, *Information Security Program*, Appendix C, paragraphs 2-201.b. (3), 3-301, and 6-601.

2.8. Processing Classified Information. The MAN is not authorized to process classified information.

2.9. Inadvertent Entry of Classified Information in the MAN. Classified information accidentally introduced into the MAN requires immediate reporting and intervention by key personnel. As a minimum, the following personnel will be notified: the FSA, UCM, unit security manager, and unit DAA. The UCM will notify the WIAO who will in turn notify the NCC, 43 CS/CC and HQ AMC Network Operations and Security Center. NCC personnel will follow locally established procedures for purging classified information from the MAN. See **Attachment 6** for instructions on partial sanitation procedures.

2.10. Sensitive Information.

2.10.1. User Responsibility. It is the responsibility of each user to properly protect and safeguard all sensitive information under his or her control. Sensitive information is discussed in para **1.6.1.**, and defined in AFMAN 33-270. Please note that the aggregation of information can result in the creation of sensitive data. For those occasions when guidance is needed to determine if specific information is sensitive or not, contact 43 CS/SCBIR (Records Management, 394-2606).

2.10.2. Storage. The preferred method of storing sensitive information is to use removable storage media, such as floppy diskettes. However, sensitive information may be stored on the "C" drive. If you choose to store sensitive information on the "C" drive, the user must take the appropriate security measure to protect that information (i.e. ensure that the folder is not shared).

2.10.3. Aggregate Data. When storing data on the MAN, each user must be careful to avoid collecting or grouping independent information where the sensitivity of the whole is greater than the sensitivity of the parts, potentially creating data not authorized for use on the MAN. In no case

will users aggregate data for placement on the MAN when any portion of the data taken individually, or taken as a whole, would be considered "classified." Users should also limit use of sensitive information on e-mail systems accessed through the MAN. Individual users should consult with their system program or functional managers to determine when issues regarding aggregated data arise.

2.11. Remanence Security. Remanence security is the control of residual information that remains on magnetic computer storage media after erasure by standard program utilities such as the DOS delete operation.

2.11.1. Remanence Security Philosophy. Sensitive information must be protected from unauthorized recovery of previously deleted data. This is accomplished by using either the remanence security process of clearing or purging. There are 3 methods by which this may be accomplished. (1) Use approved software to clear the information. To find out if your software is approved check with the WIAO or review the current Air Force approved products list. This is located on the AF Communications Agency Web page (www.afca.scott.af.mil/ip/compusec/pap/paprog.htm) (2) Use a Type I degausser. (3) Destroy the magnetic storage media. Either method two or three must be used whenever the use of method one is not possible, such as when a hard drive is not operational. See AFSSI 5020, *Remanence Security,* for additional information on clearing and purging magnetic storage media.

2.11.2. When to Clear Computer Magnetic Storage Media. Users and UCMs will clear magnetic storage media under their control that contain unclassified or sensitive information before reutilization or release from user control. Information owners will review files for record management disposition requirements prior to clearing the files from the magnetic storage media.

2.11.2.1. Users and UCMs will clear magnetic storage media (hard disks and floppy diskettes) whenever the media is reallocated to another work center or is no longer needed in the performance of official duties. Clearing is not required when an employee leaves an office and the workstation remains under the control of the functional organization.

2.11.2.2. User workstations and MAN core servers do not require clearing of sensitive information when NCC personnel perform equipment maintenance. If NCC personnel cannot repair the equipment, the NCC will notify the equipment user that vendor maintenance is required. Prior to sending a workstation to vendor maintenance, the hard drive files will be reviewed by the user to determine if sensitive information has been stored on the hard drive. If sensitive information is found, either the hard drive must be removed or those files containing sensitive information must be cleared. Prior to sending file servers to vendor maintenance, the file server hard drive will either be removed or all data files must be cleared to prevent the inadvertent release of sensitive information.

2.11.2.3. UCMs or FSAs will clear file server directories and the associated files assigned to individual users when the user departs the organization, or when the user no longer requires access to the file server to perform official duties.

2.12. Security Training.

2.12.1. Initial and Refresher User Security Training. All new users will receive initial Security Awareness Training and Education (SATE) training within 30 days of being authorized access to the MAN. This will be accomplished using the Information Assurance Computer Based Training (IACBT) available on the WIAO Web page (popenet/iacbt). The UCM will certify training has

been completed and sign the 43 AW MAN User Agreement (**Attachment 2**). Failure to do so within 30 days will result in the account being disabled. Regardless of the date of the initial training, annual refresher training will be accomplished each year in February during Information Assurance Awareness Month.

2.13. Certification and Accreditation (C&A).

2.13.1. Definition. Certification and Accreditation provides users with an assurance the system possesses adequate computer security. Accreditation is defined as the formal declaration by a Designated Approval Authority (DAA) that an information system is approved to operate in a particular security mode using a prescribed set of safeguards with an understanding of existing threats and risk. Certification is defined as the comprehensive evaluation of the technical and non-technical security features and countermeasures of an information system and other safeguards, made in support of the accreditation process. The objective of computer security is to protect information and resources so the organization can effectively accomplish its goals. To achieve this objective three important goals must be met:

2.13.1.1. Confidentiality. This ensures that only people with the appropriate clearance and the need-to-know have access to information. Confidentiality targets the prevention of disclosing information to unauthorized people.

2.13.1.2. Integrity. Integrity ensures the information people have is correct and has not been deliberately or unintentionally altered. Integrity targets the prevention of information corruption.

2.13.1.3. Availability. Availability augments the two previous goals by ensuring the availability of reliable resources to the users with the clearance and the need-to-know. Availability targets the prevention of denial of service for authorized users.

2.13.2. Responsibilities. The Designated Approval Authority (DAA) accredits all systems under their control. On Pope AFB the 43 CS/CC is the DAA for the Pope MAN and each Squadron Commander and/or directorate is the DAA for all systems within their unit.

2.13.2.1. AMC Form 1014. Use the AMC Form 1014, **System Certification and Accreditation Statement,** to document accreditation of all information systems. Preparation instructions may be found in AMCI 33-202V1.

2.13.2.2. Approval Process. Once the Certification Official (normally the UCM) and the DAA have signed the AMC Form 1014, it will be brought to the Wing Information Assurance Office (WIAO). Personnel in the WIAO will ensure that the form has been completed properly and that the information systems will be operated in a secure manner. They will also review the latest Internet Security Scan for the unit and will not approve any C & A package until all current vulnerabilities have been removed. The WIAO will annotate approval by signing the AMC Form 1014, and assigning an Accreditation Control Number (ACN) to the systems listed on the accreditation package. The ACN will be entered into the Information Processing Management System (IPMS). Systems must have an ACN assigned prior to being placed in operational use.

2.13.2.3. Reaccreditation. Evaluate changes to system architecture on a continuing basis to maintain system accreditation and ensure system modifications do not create new vulnerabilities. Systems will be reaccredited whenever system modification warrants or every three years

whichever comes first.

2.14. Internet Fraud, Waste, and Abuse (FWA) Reporting Procedures. All users must report potential security violations or other incidents to their UCM. UCMs will determine the appropriate level of notification IAW AFSSI5021, Table 1, for individual incidents. Non-COMPUSEC incidents may fall under the jurisdiction of other programs for investigation and reporting purposes. Examples include inadvertent disclosure of classified information (may or may not involve compromise); theft of information or information systems resources; Internet fraud, waste, and abuse (FWA), and copyright violations. You may use AF Form 102, **Inspector General Complaint Data Collection**, for reporting to the IG, or you may call the hotline at DSN 223-5030, toll free 1-800-424-9098. You may also use AF Form 635, **USAF Fraud, Waste, and Abuse Disclosure**, for reporting FWA incidents to the AFOSI. Unit commanders will be notified of any FWA incidents. Keep in mind the UCM may play an active role in the investigation and correction after the fact.

2.15. Personally Owned Computers. Personal computers owned by Air Force members, government employees, or contractor personnel will not be used to process classified information. Personally owned computers will not be connected to the MAN. The use of personally owned computers at work is strongly discouraged, however, it may be used for processing unclassified and sensitive but unclassified (SBU) information with DAA approval. In this case, written DAA approval will specify the conditions under which the computer will operate and the duration of the approval. If the personally owned computer is used outside of the work area, government-owned SBU information must remain on removable media and be marked and protected accordingly. Using personally owned computer hardware and software for official business should be a last resort and actions should be taken to preclude their use.

2.16. Internet and World Wide Web.

2.16.1. The multi-media resources available on the Internet and World Wide Web (WWW) have greatly increased the number of locations to seek and obtain information that can be used in our daily jobs. HQ Air Force, AMC and almost every Air Force base uses WWW sites to disseminate information about a variety of topics. This information explosion has been even greater in the commercial sector, with WWW sites available from every conceivable topic. Unfortunately, many of these sites contain inappropriate material.

2.16.1.1. The policy for using government equipment and services has not changed over the years, but needs to be reiterated with this new media in mind. Government computers, networks and telephone systems are provided for official government business and authorized use only. No personal or commercial use is authorized. Using the Internet for transacting business, or viewing entertainment, shopping, or adult oriented information is not authorized and may result in administrative or disciplinary actions.

2.16.1.2. The Communications Squadron will block access to those sights identified as unauthorized, offensive or illegal. Individual users of the Pope MAN who may inadvertently access a site that should be blocked will immediately notify their UCM who will in turn notify the WIAO.

2.16.2. Configuring a Workstation as a Web Server. Some programs delivered as part of a standard workstation software package have the ability to convert a workstation into a Web Server. Workstations configured as Web Servers may create additional vulnerabilities to a user's personal data and the MAN. Workstations will not be converted into a Web Server unless it meets the

requirement in AFI 33-129, *Transmission of Information via the Internet*, and has been approved by the DAA in writing.

2.17. Two Accounts for Persons with MAN Supervisor Privileges. Personnel who have a MAN account with supervisor privileges (including FSAs, UCMs, and Wing IA personnel) will have a second account with user-only privileges established. Personnel will log-in with supervisor privileges only when performing supervisor tasks. At all other times, they will log-in via the second account as a regular MAN user.

2.18. Air Force Computer Emergency Response Team (AFCERT) Advisories. These advisories identify specific software and operating system vulnerabilities. By naming affected platforms and making recommendations for corrections, patches, or workarounds, the vulnerability of applicable named systems is minimized to an acceptable level. UCMs will receipt for each advisory and coordinate with FSAs within their unit to ensure the corrective actions to each vulnerability, as recommended in the AFCERT advisory, is immediately implemented. Furthermore, the UCM will receipt for every AFCERT advisory within 24 hours of receipt, by e-mail, to the Wing IA office. Upon implementation of the recommended solution, the UCM will immediately inform the IA office of what action was taken. If immediate implementation of the corrective action is not possible, provide Wing IA with a weekly status report on what action is being taken to comply with the advisory. The Wing IA office will consolidate all unit responses and forward a summary report to HQ AMC IAC. Each UCM will maintain a log or database (electronic or paper) of all advisories and the status of their implementation. If an advisory is not applicable, simply annotate the log as such. The IA office will also file unit responses and update its AFCERT database with actions taken. See AMCI 33-202, Volume 1, *Information Assurance*, paragraph 6.2, for information on security advisory registration, implementation, and tracking.

3. Information Assurance Assessment and Assistance Program (IAAAP).

3.1. General. The IAAAPs purpose is to “find and fix” wing-level information assurance problems. The IAAAP accomplishes this by:

3.1.1. Assessing IA programs, the security posture of wing information systems, and the information contained within the systems.

3.1.2. Identifying and recommending solutions.

3.1.3. Helping to resolve problems.

3.1.4. Providing technical and training assistance including instructions in system accreditation and system policy development, when possible.

3.2. Responsibilities.

3.2.1. Wing Information Assurance Office.

3.2.1.1. Perform semiannual assessment of Wing IA operations. This will include COMSEC, COMPUSEC, EMSEC and SATE. AFCOMSEC Form 13 will be used to conduct this assessment and will be conducted in March and September of each year.

3.2.1.2. Conduct random, unannounced site visits.

3.2.1.3. Provide squadron commanders with a written assessment of their IA posture, to include commendable areas, outstanding personnel and recommended improvement areas.

3.2.1.4. Provide assistance in correcting any discrepancies.

3.2.1.5. Provide the 43 AW Commander a written report detailing the overall IA posture of the base. This will be done using the Pass/Fail Criteria designated on the AFCOMSEC Form 13.

3.2.1.6. Serve as the final authority on determining the adequacy of unit responses to IAAAPs and closing of individual deficiencies or reports.

3.2.2. Unit Responsibilities.

3.2.2.1. Conduct self-assessments of Unit IA programs and correct deficiencies as necessary.

3.2.2.2. Ensure that responsible officers have been appointed for each program (as required) in their unit. Ensure that appointment letters are current.

3.2.2.3. Ensure program responsible officers are provided sufficient training for their duties.

3.2.2.4. Facilitate program reviews by the Wing IA office during the months of March and September.

3.2.2.5. Respond to IAAAP reports within 30 days. (Only units with identified discrepancies need respond. All others file and retain until the next MAJCOM review.

RICHARD J. CASEY, Brigadier General, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 90-301, *Inspector General Complaints*

AFI 33-119, *Electronic Mail (E-Mail) Management and Use*

AFI 33-129, *Transmission of Information via the Internet*

AFI 33-132, *Air Force Privacy Act Program*

AFI 33-202, *Computer Security*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFMAN 33-223, *Identification and Authentication*

AFSSI 5001, *Security Policy Development Guide*

AFSSI 5020, *Remanence Security*

AFSSI 5021, *Vulnerability and Incident Reporting*

AFSSI 5024, Volume I, *The Certification and Accreditation Process*

AFSSI 5024, Volume II, *The Certifying Official's Instruction*

AFSSI 5027, *Network Security Policy*

AFSSM 5023, *Viruses and Other Form of Malicious Logic*

AMCI 33-202, Volume 1, *Information Assurance*

DoD 5200.1-R, *Information Security Program*

Abbreviations and Acronyms

ADPE—Automated Data Processing Equipment

AFCERT—Air Force Computer Emergency Response Team

AFI—Air Force Instructions

AFSSI—Air Force Systems Security Instructions

AFSSM—Air Force Systems Security Memorandum

APL—Assessed Product Listing

C&A—Certification and Accreditation

COMPUSEC—Computer Security

CSRD—Communications-Computer Requirements Document

CSSO—Computer Systems Security Officer

DAA—Designated Approving Authority

ECO—Equipment Control Officer

E-MAIL—Electronic Mail

FSA—Functional System Administrator

FWA—Fraud, Waste, and Abuse

IA—Information Assurance

IPMS—Information Processing Management System

MAN—Metropolitan Area Network

NCC—Network Control Center

NCSC—National Computer Security Center

PUID—Personal User Identification

SBU—Sensitive but Unclassified

UCM—Unit COMPUSEC Manager

WIAO—Wing Information Assurance Office

WGM—Work Group Manager

Attachment 2

METROPOLITAN AREA NETWORK USER AGREEMENT & PERSONAL USER ID (PUID) RECEIPT

1. I declare an official duty requirement for an account on the Pope Metropolitan Area Network (MAN). I will comply with all operational and security guidance issued by the base Network Control Center (NCC), Wing Information Assurance (IA) personnel, and Functional System Administrator. I will report any deviations from prescribed computer security provisions to one of the above personnel. I will abide by these rules for all government systems to which I have access.

2. I agree to adhere to the following procedures as an authorized user of the 43d Airlift Wing Metropolitan Area Network (43 AW MAN):

I am responsible for all activity that occurs under my User ID. I will protect my password to prevent unauthorized disclosure. I will change my password every 90 days or as directed.

I will not automate the entry of my password.

I will safeguard all sensitive data and resources. I will mark output products appropriately (FOUO, Privacy Act, etc.). I will not release sensitive information to personnel without the proper clearance, access, or need-to-know.

I will not introduce or process classified information on the MAN.

I will comply with the provisions outlined in AFI 33-119, *Electronic Mail (E-Mail) Management and Use* and AFI 33-129, *Transmission of Information via the Internet*. The following is a brief summary of prohibited activities:

I will not use government hardware and software for other than official business (Using for personal or financial gain, chain letters, subscribing to unofficial mail lists, sales of personal property, etc.).

I will not access, store, process, display, or transmit offensive or obscene language or material. This includes, but is not limited to, racially offensive material or symbols and sexually explicit materials.

I will not store or process copyrighted material. This includes obtaining, installing, copying, or using software in violation of the appropriate vendor's license agreement.

I will not participate in "chat line" or open forum discussion for other than official purposes.

I will not make any configuration changes or modifications to system hardware or software, or take any action to alter connectivity or interface to the network without permission.

I will not use another person's account or identity without authorization or permission.

I will not intentionally misrepresent my identity or affiliation in e-mail communications.

I will not attempt to circumvent of defeat security mechanisms or auditing systems.

I will not permit unauthorized individual(s) access to a government-owned or operated system.

I understand that the 43 AW MAN is subject to monitoring at all times as stated in the following statement:

This is a Department of Defense computer system. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored.

Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes."

I will not add any software or hardware to the system without authorization from my Designated Approving Authority (DAA) who is _____.

I understand that I am not allowed to view/place computer games or pornography on official government systems, or to use official government systems for personal financial gain.

I will not install any freeware or shareware on my computer without the written permission of the DAA and the Wing Information Assurance office.

If I have an Internet Protocol (IP) address, which allows access to the Internet, I will not change it, nor will I attempt to enter any sites using any form of Web Protocol that are in violation of AFI 33-129.

I know it is a security violation for any user to mask their identity or use the identity of another user.

I know this system is for unclassified and sensitive unclassified information (Privacy Act and FOUO).

I will not enter data into the system if the data is of a higher classification level than the system.

Only authorized personnel are authorized access to my computer.

I will not release government information to the public unless authorized.

I will report any suspected instances of fraudulent or unauthorized practices or use immediately to my immediate supervisor or through the procedures stated in AFI 90-301, *Inspector General Complaints.*

I agree to follow my office security procedures, official regulations, and policies applicable to information system operations. This certificate is only a short summary to stress key points. I understand I am subject to disciplinary action under the UCMJ or applicable criminal or civil sanctions for civilian personnel for any violation of operating procedures or abuse of access privileges.

3. I understand this is only a brief summary of applicable procedures and polices for operating government computers and networks. I will operate the system IAW established security directives and procedures. I will comply with all the provisions of this agreement.

4. I understand this agreement and acknowledge receipt of my user ID and password. I agree to complete Security Awareness Training and Education (SATE) Computer Based Training (CBT), within 30 days of this receipt. I will have my UCM sign off on this letter verifying that I have completed this training. Failure to do so will result in disabling of this account.

_____	_____
LOGON (User ID)	UCM Verification of Training
_____	_____
Last, First, Middle Initial	Rank/Grade
_____	_____
Organization/Office Symbol	Phone
_____	_____
Date	Signature

Attachment 3

LOGIN BANNER

The Pope AFB MAN and each information system will display the following login banner. [Source: AFI 33-219, *Telecommunications Monitoring and Assessment Program* (TMAP), para A2.3.5, dated 1 June 1998.]

This is a Department of Defense computer system. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored.

Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes."

Attachment 4

MALICIOUS LOGIC INCIDENTS

The following is the format to be used when reporting malicious logic incidents. Requests for assistance in filling out this form should be directed to the unit FSA or UCM. If necessary, contact the Wing Information Assurance Office (394-2262/2627) for further assistance.

VIRUS INCIDENT REPORT

1. Date Reported: _____

2. Report Individual Information:
a. Rank/Name_____
b. Organization_____
c. DSN Phone_____
d. E-mail Address_____

3. Date of Incident: _____

4. Virus Name:_____

5. Operating System: _____
Version #:_____

6. Anti-viral Tool/Software Used:_____

7. Is the Information System Mission Critical?
Yes No

8. Impact *(Choose all that apply)*:
a. Data Alteration
b. Denial of Service
c. Data Integrity
d. None

9. Number of Systems Infected:_____
Number of Floppies Infected:_____
Network/IP:_____

10. Work-Hours Lost:_____

11. Fix Action:
a. Rebuilt System
b. Eradicated Virus
c. Destroyed Floppy

12. Mission of Computer/Impact of Virus on Mission:_____
_____
_____
_____
_____

_____

13. Damage Observation:_____

_____

_____

_____

14. Source of Infection:_____

Attachment 5

INSTRUSION INCIDENTS

The following is the format to be used when reporting intrusion incidents. Requests for assistance in filling out this form should be directed to the unit UCM or FSA. If necessary, contact the Wing Information Assurance Office (394-2262/2627) for further assistance.

INITIAL INTRUDER REPORT

1. Report Date:_____

2. Report Originator Information:
   a. Rank/Name_____ f. E-mail Address_____
   b. Unit/Base_____ g. Message Address_____
   c. DSN Phone_____ h. Mailing Address_____
   d. Position_____
   e. MAJCOM_____

3. Target Information *(Additional targets need separate sheet)*:
   a. Network Domain Name_____
   b. IP Address_____
   c. Computer Model (i.e., Sparc 5)_____
   d. Operating System/Version_____
   e. Security Mode of Operation_____
   f. Network/System Mission_____
   g. Security Classification_____
   h. Network Structure/Type_____
   i. How Detected_____
   j. Impact on Mission_____
   k. Information System Auditing_____

4. Attack Session Information *(Correlates with the target information)*:
   a. Date(s) of Session_____
   b. Time_____

c. Attack Method_____

d. Success_____

e. Account *(Include host name if available)*_____

f. First Layer Point of Origin_____

5. Brief Scenario *(Description of incident)*:_____

_____

_____

_____

_____

_____

6. Countermeasure(s) Installed:_____
   Name and Date Installed:_____

7. Notifications *(Indicate name, date, and time notified)*:
   a. UCM_____
   b. Wing Information Assurance Office_____
   c. MAJCOM Information Assurance Office_____
   d. AFCERT_____

Attachment 6

VULNERABILITIES

The following is the format to be used when reporting vulnerabilities. Requests for assistance in filling out this form should be directed to the unit UCM or FSA. If necessary, contact the Wing Information Assurance Office (394-2262/2627) for further assistance.

VULNERABILITY REPORT

1. Report Date:_____

2. Report Originator Information:

a. Rank/Name_____ f. E-mail Address_____

b. Unit/Base_____ g. Message Address_____

c. DSN Phone_____ h. Mailing Address_____

d. Position_____

e. MAJCOM_____

3. Description of Technical/Administrative Vulnerability:

(Describe the nature and effect of the vulnerability. The description should sufficiently reconstruct the computing environment so you can repeat the flaw without further information. Describe codes or procedures discovered that might reduce the impact of the vulnerability.)

_____

_____

_____

_____

_____

_____

_____

4. Impact *(Choose one)*:

a. Denial of Service_____

b. Integrity_____

c. Compromise_____

d. Others *(Fully explain)*_____

5. Hardware and Software Information:

a. CPU Model_____

b. Configuration *(Indicate if the Information System is a workstation or stand-alone)*_____

c. Name and Version Number of Affected Software_____

d. Security Classification_____

6. Connectivity:

a. MAN Name, MAJCOM, Unit_____

b. Attack Method_____

7. Work-Hours Lost:_____

8. Notifications *(Identify vendors, developers, and COMPUSEC individuals notified)*:_____

_____

_____

_____

_____

_____

Attachment 7

SANITATION PROCEDURES

To permanently delete e-mail (limited procedures):
Build a new PST file
Add to Outlook Client profile
Copy all folders and messages into new PST on server
Remove old PST from profile
Delete old PST from system
Defragment the system (if Windows 95)
If attachments are involved, wipe unallocated disk space with approved software
Partial Sanitation
Wipe unallocated disk space with approved software
Back-up all user files
Format the hard drive
Reinstall the operating systems and applications
To remove all Traces of an E-mail from the Exchange Server:
Compile a list of all recipients and corresponding servers
Check to see if the Dumpster option is enabled
Check to see if the dumpster option is enabled for each recipient
Check for journaling on the server
Delete each copy of the message
Perform a full online Exchange Backup
Partial Sanitation
Perform an offline compaction of Priv.edb
Complete Sanitation
Zero wipe disk containing transaction logs
Backup the files on the disk containing the Priv.edb file
Restore all the files